Systematic government access to private-sector data in France*

Winston Maxwell**

Abstract

- In regulating access to data by law enforcement and the intelligence services, France distinguishes between different levels of government intrusions into privacy: for example, real-time interception of private correspondence, whether by telephone, e-mail or instant messaging; cloning or monitoring a computer terminal at a distance by the police; or requiring disclosure of stored computer data.
- Post 11 September 2001 France enacted provisions to require telecommunications operators and providers of hosting services to retain significant amounts of traffic data and so-called 'identification data', a requirement which implements relevant EU instruments, but tends to go beyond the retention of data required by EU law.
- France's intelligence agencies have wide-ranging powers to collect data and conduct interceptions, as indicated in recent news reports, but questions exist as to what protections, if any, exist for intelligence surveillance conducted by the authorities outside of France, as well as for 'general monitoring for radio transmissions' conducted within France or as part of general monitoring of radio transmissions.

France, like other democratic countries, distinguishes between different levels of government intrusions into privacy. The highest level of intrusion into privacy consists of real time interceptions of private correspondence, whether by telephone, e-mail, or instant messaging. For any such interception, a prior authorization of an independent judge is necessary.[1] The independent judge is either the investigating magistrate (*juge d'instruction*) or the judge of liberty and detention (*juge des libertés et de la détention*). As an exception to this rule, certain interceptions of private correspondence can occur without a judge's approval in the context of national security interceptions, untargeted national security monitoring of radio transmissions, or intelligence gathering outside of France. These exceptions will be examined in more detail below.

Another form of intrusion into privacy that is entitled to the highest level of safeguards in France is a police technique pursuant to which the police can clone and monitor at a distance a computer terminal. This technique is referred to in France as the 'capturing of computer data' and can be implemented after authorization by either an investigating judge or a judge of liberty and detention.[2] This technique authorizes police authorities to hack into a computer system and monitor in real time every key stroke of the relevant terminal. This technique can be used only for investigations into organized crime.

Other forms of access to computer data are deemed less intrusive of privacy and therefore are surrounded by fewer safeguards. Under normal rules of criminal procedure (we'll examine national security below), police authorities can require disclosure of stored computer data with varying levels of approval, depending on the stage of the investigation. If police authorities have reason to believe that a crime is in the course of being committed (*flagrance*), then an officer from the judicial police can require disclosure of computer data immediately, as long as the officer informs the public prosecutor at the same time.[3]

If the request for computer data is in the context of a preliminary investigation (*enquête préliminaire*), the public prosecutor must specifically grant authority to the judicial police to proceed with the request for computer data.[4] The public prosecutor is trained as a magistrate but

* This paper is part of the Systematic Government Access to Private-Sector Data symposium, Part 2. Part 1 can be found in *International Data Privacy Law* volume 2, issue 4.

** Partner, Hogan Lovells LLP, member of the Paris and New York bars.

1 Articles 100 and 706–95, Code of Criminal Procedure.

2 Article 706–102–1, Code of Criminal Procedure.

3 Articles 57–1, 10–1, 60–2 1, Code of Criminal Procedure.

4 Articles 77–1–1 and 77–1–2, Code of Criminal Procedure.

he or she is not a judge when acting in his or her capacity as public prosecutor. The public prosecutor is comparable to the role of a district attorney in the US legal system.

Finally, if the investigation has advanced to the stage where an investigating judge (*juge d'instruction*) is appointed, then the investigating judge must authorize all measures to compel disclosure of computer data.[5]

All of these requests for computer data, whether ordered by the judicial police, the prosecutor or investigating judge, are known under French law as *réquisitions*. The French code of criminal procedure provides that a *réquisition* requiring access to computer data can permit access to data that is stored in servers outside of France as long as the *réquisition* involves a terminal that is located in France and that has authorized access to the relevant data located abroad.[6] The location of the data is irrelevant. All forms of *réquisition* also permit access to so-called connection data and identification data stored by telecoms operators and by hosting providers under French law.

Customs authorities have separate authority to issue *réquisitions* of computer data in connection with the investigation of potential customs or tax violations.[7] These *réquisitions* may be issued by a customs official having the rank of at least 'controller', and do not need to be approved by a judge. Telecoms operators, banks, and airlines are among the kinds of companies that can receive orders from customs authorities for the communication of computer data.

The reminder of this article will focus on:

1. provisions enacted in France post 11 September 2001 to require telecommunications operators and providers of hosting services to retain significant amounts of traffic data and so-called 'identification data'; and
2. the broad-ranging powers of France's intelligence agencies to collect data and conduct interceptions.

Storage and access to traffic data and identification data

France transposed the European directive on retention of traffic data,[8] but went beyond the minimum required by the directive. French law not only requires telecommunications operators to retain traffic data (including location data and Internet logs[9]) for one year, but also requires hosting providers to retain similar logs relating to persons who create or store data using their hosting service. The definition of hosting provider is similar to that in the E-Commerce Directive,[10] and broad enough to include many cloud providers, social media services, blogs, and video sharing platforms. The hosting provider must retain all the information provided by the user when he or she registers for the service, including the user's name, pseudonym, address, telephone number, e-mail address, password, information permitting the user to change the password, and payment information.[11] When a user uploads content, the hosting provider must keep logs regarding the user's connection to the service. All the foregoing data is considered 'identification data' and is subject to government access, as described below.

There are two official ways for the French government to obtain traffic data and identification data from telecoms operators and hosting providers without the involvement of a judge, plus a third less official route identified by the French press. First, the French Internal Security Code allows the French government to request traffic data, including location data, from telecoms operators and hosting providers for any national security investigation.[12] The request does not have to be approved by a judge. However, the government must seek the prior approval of a person designated by the Prime Minister after nomination by the Commission on Security Interceptions (CNCIS), an independent commission created in 1991 to oversee national security wiretaps. (We will discuss the CNCIS and its functions in more detail below.) The number of requests made using this procedure is approximately 30,000 per year.[13]

The second and historically more popular means for the government to acquire traffic data is through a provision in the Internal Security Code[14] that permits the government to obtain from telecoms operators any information or documents that may be necessary as a preparatory matter in connection with potential national security interceptions. (We will examine 'security interceptions' in more detail in a separate section below.) For these requests for traffic data, the government does not have to involve the CNCIS, although the CNCIS can request information about the data collection after the fact. However, the request must still be cleared by

5 Articles 94 and 97, Code of Criminal Procedure.
6 Article 57-1, Code of Criminal Procedure.
7 Article 65, Customs Code.
8 Directive 2006/24/EC of 15 March 2006.
9 Decree no. 2006-358 of 24 March 2006.
10 Directive 2000/31/EC.
11 Decree no. 2011-219 of 25 February 2011.
12 Article L 246-1 of the Internal Security Code. Previously these requests were governed by provisions in the French Post and Electronic Communications Code. Those provisions are now replaced by article L 246-1 of the Internal Security Code.
13 CNCIS Annual Report for 2011-2012 (*20ème Rapport d'Activité 2011-2012*), 66. These statistics apply to the procedure that existed prior to the changes made by the December 18, 2013 law.
14 Article L 244-2, Internal Security Code.

the Prime Minister's office first. The Ministry of Interior and Ministry of Defence cannot make the requests directly without going through the Prime Minister's office. According to a recent parliamentary report,[15] the number of requests made using this method is approximately 200,000 per year, making it by far the most preferred method for obtaining traffic data through official routes. This route only permits the collection of 'traffic data' from telecoms operators. It does not permit the collection of 'identification data' from hosting providers.

The government reportedly uses a third unofficial route to obtain traffic and identification data. This route falls completely outside the scope of any supervision by the CNCIS, and was brought to light in 2010 by the newspaper *Le Canard Enchaîné*[16] after it revealed that the government had acquired traffic data to try to determine the source of leaks of confidential information from within the government to the *Le Monde* newspaper in connection with an internal political scandal. This third route is based on the government's ability to conduct generalized monitoring of radio transmissions in order to protect France's national interests. France's Internal Security Code recognizes the government's right to conduct generalized monitoring of radio transmissions outside of any supervision either by the courts or by the CNCIS.[17] The code also says that the Ministry of Interior or Ministry of Defence may request from telecoms operators any documents or other information necessary to implement such generalized monitoring.[18] As a result of the political scandal associated with alleged transfers of funds from the billionaire Liliane Bettencourt to close associates of the French president, a French intelligence agency obtained calling records from telecoms operators to try to trace the source of leaked information within the government. When questions arose regarding the government's legal basis for obtaining this traffic data, the Director of National Police responded that the data were acquired pursuant to the provision allowing the French government to conduct general monitoring of radio transmissions and to request information from telecoms operators relating to such monitoring.[19] The concept of general monitoring of radio transmissions is not defined in the Internal Security Code. Parliamentary debates show that the concept is intended to cover 'random sweeping of radio transmissions, without targeting ahead of time any individualized communications'.[20] Radio transmissions are not defined, but would generally include cell phone, satellite, and WiFi communications.

Le Canard Enchaîné also obtained an internal governmental memorandum dated February 17, 2010 indicating that for requests of traffic data on this basis (information needed for general monitoring of radio transmissions), the Ministry of Defence or Ministry of Interior did not have to go through the Prime Minister's office first, but could address their request directly to the telecoms operators. These requests also are not reviewed at any time by the CNCIS. According to *Le Canard Enchaîné*, the CNCIS had seen and approved this governmental memorandum in a meeting dated 21 January 2010, although two of the three members of the CNCIS denied having any knowledge of it. According to *Le Canard Enchaîné*, this procedure basically opens an 'all-you-can-eat buffet' for France's intelligence agencies to obtain traffic and communications data from operators without any supervision either from the Prime Minister's office, or from the CNCIS. A 14 May 2013 parliamentary report indicates that as a result of the 2010 scandal, the Prime Minister's office published a memorandum stating that article L 241–3 of the Internal Security Code cannot be used to collect personal data.[21] It is not known whether this third unofficial route is still used, and to what extent. On 5 July 2013, *Le Monde* indicated that France's external intelligence agency, the DGSE, still collects large volumes of data:

> [The DGSE] collects telephone data of millions of subscribers—the identifier of the calling parties, of the called parties, the place, date, duration and size of the message. The same thing exists for e-mails (with the possibility to read the subject line of the e-mail), SMSs, faxes . . . and all Internet activity that goes through Google, Facebook, Microsoft, Apple, Yahoo! . . . This is what the parliamentary delegation for intelligence calls 'electromagnetic intelligence gathering' (ROEM), which is the translation of Sigint (signal intelligence) of the NSA.[22]

The recent parliamentary report on the reform of France's intelligence agencies[23] recommends that French law be reformed so that only one procedure exists for the

15 National Assembly, Report No. 1022 of 14 May 2013 on the review of the legal framework applicable to intelligence services, p. 24.

16 Didier Hassoux and Hervé Liffran, 'La loi sur les écoutes trafiquée à Matignon', *Le Canard Enchainé*, 29 September 2010, 3.

17 Article L 241–3, Internal Security Code.

18 Article L. 244–2, Internal Security Code.

19 National Assembly, Report no. 1022 of 14 May 2013, 25.

20 Statement of French Minister of Justice during the parliamentary debates surrounding the 1991 law. *Assemblée nationale, compte rendu intégral, séance du jeudi 13 juin 1991, J.O. du 14 juin 1991*, 3124.

21 National Assembly, Report no. 1022 of 14 May 2013, 25.

22 Jacques Follorou and Franck Johannès, ' Révélations sur le Big Brother français', *Le Monde*, 5 July 2013.

23 National Assembly, Report No. 1022 of 14 May 2013, 24.

collection of traffic data for national security reasons, and that all requests for data be approved by the CNCIS. According to the report, having multiple procedures permits agencies to pick and choose the procedure that is the most convenient for them, including procedures that involve no supervision either by a court or by the CNCIS.

18 December 2013 law facilities real-time data collection

French law was reformed on 18 December 2013, via a law on military spending[24] which contains two provisions that facilitate the collection of data by the French military and intelligence services. The first provision relates to the collection of passenger name records (PNRs). Under the new law, airlines are required to send PNRs to authorities in accordance with a yet to be adopted government decree. The data may be held for up to five years and may not contain sensitive data: i.e., data relating to the passenger's racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union menbership, health, or sexual orientation. The French data protection authority, the CNIL, was consulted in connection with these new PNR provisions.

The second and more controversial government data collection provision is article 20 of the 18 December law that permits French intelligence and secutity agencies to collect metadata from telecom operators and hosting providers, including in real time if necessary. The request must first be cleared by the Prime Minister's office, by a person specially named by the Prime Minister after nomination by the CNCIS. Security officials can request real-time access to metadata for reasons linked to terrorism, national secutity, and defense of France's economic and scientific potential. The requests are not reviewed by a court. However, the CNCIS is informed within 48 hours afterwards, and can then make recommendations to the Prime Minister, such as suggestions to discontinue data collection or to limit its scope. The CNCIS's recommendations are not binding.

This second provision of the 18 Decmber law attracted controversy, in part because France's data protection authority, the CNIL, was not consulted. The CNIL publised its concerns about the new law on 20 December, indicating that the terms of the law seemed broad enough to cover content data, and not just traffic data. The CNIL said that the Chairman of the Senate's Commission on Laws had indicated that the real-time collection of metadata would only concern location data. (This does not appear clear from the wording of the law.) The CNIL also said that it believed that the text would not result in massive, vaccum-cleaner type, collection because the collection mechanism would be controlled by the network operators. The CNIL said it will be "extremely vigilant" in connection with the government decrees that are necessary to implement the law.

Security interceptions

Prior to 1991, France had no specific statute dealing with wiretaps. Wiretaps were authorized by investigating judges based on those judges' general authority to conduct investigations. No statute defined exactly which crimes could justify a wiretap, and under what conditions the wiretap could be performed. Similarly, France had no statutory framework for so-called 'administrative' wiretaps conducted by government officials without court order, generally for national security reasons. In *Kruslin v France*,[25] the European Court of Human Rights found that the absence of a statutory framework for wiretaps in France violated article 8 of the European Convention of Human Rights, because the wiretaps in France were not 'in accordance with law'. The court held that the term 'in accordance with law' requires a statute with specificity on how wiretaps are conducted, what crimes justify a wiretap, how long recordings are held, and who can have access to them. France's regime on wiretaps before 1991 was based on case law, which over the years had built in safeguards limiting the use of wiretaps by investigating judges. The use of administrative national security interceptions was governed by an internal and confidential government circular from 1961. France's extensive use of wiretaps without court order had been a source of concern for lawmakers, particularly after a confidential report prepared in 1982 by a parliamentary commission lead by Robert Schmelck.[26] The European Court of Human Rights had also found Germany's[27] and England's[28] laws deficient.

On 10 July 1991 France adopted a wiretap law, which today still forms the basis for police interception of communications.[29] The 1991 law deals with both judicial interceptions for the purpose of investigating crimes,

24 Law no. 2013-1168 of 18 December 2013.

25 *Kruslin v France*, ECHR 11801/85, 24 April 1990.

26 Claudine Guerrier, 'Etude de droit compare en matière d'organismes de contrôle pour le interceptions téléphoniques', Working Paper Télécom & Management, January 2009, p. 10.

27 *Klass v Germany*, ECHR 5029/71, 6 September 1978.

28 *Malone v United Kingdom*, ECHR 8691/79, 2 August 1984.

29 Law no. 91-646 of 10 July 1991.

and interceptions conducted by the government without court order for national security reasons. The latter are called 'security' interceptions. The provisions on judicial interceptions have now been inserted into France's Code of Criminal Procedure. As noted in the first part of this article, wiretaps conducted under the Code of Criminal Procedure require a prior court order. The provisions on 'security' interceptions have now been inserted into France's Internal Security Code.

The 1991 law on interceptions created an institutional framework for 'security interceptions'. Authorities may intercept any kind of electronic communication: telephone, e-mail, instant message, SMS, and data transmissions. Interceptions can also include communications that merely transit through France.[30] The interceptions are requested by the Ministry of Interior or by the Ministry of Defence, and authorized by specially-named persons in the Prime Minister's office. The reasons that can justify a 'security' interception are:

> seeking information relating to national security, safeguarding essential elements of France's scientific and economic potential, or preventing terrorism or organized crime, or the recreation or maintenance of groups that have been dissolved under the law of January 10, 1936 on combat groups and armed militia.[31]

During the parliamentary debates leading up to the 1991 Law, certain members of parliament questioned the broad terms used in the law, particularly the justification 'safeguarding essential elements of France's scientific and economic potential', which could allow purely economic spying. Others criticized the inclusion of organized crime in the scope of the 1991 law, because including organized crime seemed to create an overlap with the responsibilities of the police and the judicial branch who investigate crimes. There was concern that the police could use 'security interceptions' as a short-cut to avoid more burdensome judicial procedures.[32] These objections were set aside, and today the French framework for national security allows the interception of communications without a court order for a broad range of national security reasons, including purely economic espionage.[33]

The CNCIS

The 1991 law created two separate safeguards. First, requests for security interceptions must be cleared by the Prime Minister's office. Second, the law created a separate commission with responsibility for overseeing national security interceptions. The 'Commission on Security Interceptions' (*Commission Nationale de Contrôle des Interceptions de Sécurité*, or CNCIS) consists of three people: one person named by the French President, one person named by the chairman of the National Assembly, and one person named by the chairman of the Senate. When the Prime Minister's office grants approval for a national security interception, the interception may proceed but the Prime Minister's office must inform the chairman of the CNCIS within 48 hours. If the chairman of the CNCIS feels that the authorization granted by the Prime Minister's office does not comply with the 1991 law, the chairman can consult the other two members of the Commission and then send a non-binding recommendation to the Prime Minister's office requesting termination of the interception or modification of its terms. The decisions of the CNCIS are secret, but every year the Commission publishes a report to Parliament. While the Commission cannot go into detail about any particular security interception, the Commission can and does comment on the number of interceptions requested,[34] and the reasons therefor. The Commission also indicates the number of requests that raised problems for the Commission and for which the Commission sent recommendations back to the Prime Minister.

When the 1991 law was being debated at the National Assembly, some members of Parliament were troubled by the fact that the CNCIS did not include any judges. Because interceptions constitute a significant invasion of privacy, some members of Parliament felt that not having any judges on the Commission would make the French system illegal under the European Convention on Human Rights. The French *Conseil d'Etat* reviewed the 1991 law before it was enacted, and concluded that the procedural safeguards put into place by the Commission were sufficient to protect individual rights. However, the issue has not been directly addressed by the European Court of Human Rights.

As noted above, intelligence agencies have authority to collect traffic data from telecoms operators by alleging that the data are necessary in connection with a potential security interception. Approximately 200,000 such requests are made per year, and they are not reviewed by CNCIS. Under another procedure described earlier in this article, intelligence agencies can request

30 Court of Cassation, Criminal Chamber, Decision of 1 February 2011.

31 Article L 241-2, Internal Security Code.

32 Assemblée nationale, Compte rendu integral, 1ère séance du jeudi 13 juin 1991, J.O. du 14 juin 1991.

33 For anecdotes relating to economic espionage, see 'Paris en pointe dans la guerre de l'ombre entre alliés', *Le Monde*, 5 July 2013.

34 According to the CNCIS annual report for 2011-2012, 6,341 security interceptions were requested in 2011. *CNCIS, 20ème rapport d'activité 2011-2012*, p. 58.

traffic data from telecoms operators or identification data from hosting providers, but must seek the approval of a person specially named by the Prime Minister's office. The number of such requests is approximately 30,000 per year. Under France's new law, intelligence agencies can obtain traffic data in real time.

Intelligence gathering outside of France purportedly falls outside of French legal constraints

The 14 May 2013 parliamentary report on the legal framework for French intelligence services recommends the transformation of CNCIS into a commission with broader authority over intelligence-gathering, and that the new commission approve intelligence gathering missions in advance, taking into account legal criteria flowing from the case law of the European Court of Human Rights.[35] Interestingly, the parliamentary report states that intelligence gathering outside of France should continue to fall outside the provisions of French law and be subject only to 'international law constraints'.[36] This confirms the allegation made by Le *Monde* newspaper in its 11 June 2013 article on France's collection of data and monitoring of communications.[37] According to *Le Monde*, France's intelligence agencies take the position that their collection of data outside of France does not fall under French legal constraints. Consequently, French intelligence services allegedly collect massive amounts of data from various listening stations outside of France, including one in Djibouti,[38] and these collection activities do not involve any supervision by the CNCIS, the Prime Minister, or anyone else. Journalists and security specialists have referred to France's global listening infrastructure as France's 'big ears', or 'Frenchelon', in reference to the NSA's 'Echelon' programme.[39] The data collected from these listening stations allegedly includes data from both satellites[40] and submarine cables.[41] The data are then centralized in large data centres located in Paris.[42] These activities are conducted without any supervision by the CNCIS. The 14 May 2013 parliamentary report proposes not to change this. According to the report, intelligence gathering outside of France must remain outside of internal legal constraints, because of their clandestine nature.[43] The report proposes that provisions of a new law expressly confirm the principle of non-applicability of French law, to avoid ambiguity. The same report also recommends that 'classified' operations not be subject to prior authorization by the future commission, because those operations are 'manifestations of national sovereignty'.[44] These recommendations were not acted on in the 18 December 2013 law.

General monitoring of radio transmissions is permitted without supervision.

Article L 241–3 of the French Internal Security Code recognizes a broad exception for general monitoring of radio waves for 'defending national interests'. As noted above in connection with the collection of traffic data, the French Internal Security Code permits 'random sweeping of radio transmissions, without targeting ahead of time any individualized communications'.[45] Radio transmissions may include cell phone, satellite, or WiFi communications. Generalized monitoring of radio transmissions may be conducted without any authorization or *ex post* supervision.[46] According to the Minister of Justice in 1991, 'such measures cannot be considered as a violation of the secrecy of correspondence', although the Minister did not explain why he reached this conclusion.[47] Article L 244–2 of the Internal Security Code states that telecommunications operators must provide to the Ministry of Defence or Ministry of Interior any 'information or documents' necessary for the implementation and exploitation of 'interceptions' authorized by law. The term 'intercep-

35 Report No. 1022 of 14 May 2013 on the review of the legal framework applicable to intelligence services, p. 66.

36 *Id.*, p. 44.

37 *Le Monde*, 'En France, la DGCSE au coeur d'un programme de surveillance d'Internet', 11 June 2013.

38 Jean-Marc Manach, Bug Brother, 'La DGCSE a le « droit » d'espionner ton Wi-Fi, ton GSM et ton GPS aussi', 11 July 2013, Le Monde Blogs.

39 Kenneth Cukier, 'Frenchelon: France's Alleged Global Surveillance Network and its Implications on International Intelligence Cooperation', working paper presented at Computers, Freedom & Privacy 99 Conference, 6 April 1999; Jean Guisnel, 'Les Français aussi écoutent leurs alliés', *Le Point*, 6 June 1998, modified 25 January 2007; Jean-Marc Manach, 'Frenchelon: la DGSE est en « 1ère division »', blog.lemonde.fr, 2 October 2010.

40 Vincent Jauvert, 'Le DGSE écoute le monde (et les français) depuis plus de trente ans', *Le nouvel observateur*, 4 July 2013.

41 Jean-Marc Manach, 'La DGSE a le 'droit' d'espionner ton Wi-Fi, ton GSM et ton GPS aussi', blog.lemonde.fr, 11 July 2013.

42 *Id.*

43 Report No. 1022 of 14 May 2013 on the review of the legal framework applicable to intelligence services, p. 44.

44 *Id.*, p. 69.

45 Statement of French Minister of Justice during the parliamentary debates surrounding the 1991 law. *Assemblée nationale, compte rendu intégral, séance du jeudi 13 juin 1991, J.O. du 14 juin 1991*, p. 3124.

46 There may exist internal guidelines, but they are not public.

47 Statement of French Minister of Justice during the parliamentary debates surrounding the 1991 law. *Assemblée nationale, compte rendu intégral, séance du jeudi 13 juin 1991, J.O. du 14 juin 1991*, p. 3124.

tions' refers in this section not only to security interceptions, but also to the generalized monitoring of radio transmissions permitted by article L 241–3 of the Internal Security Code. The generalized monitoring therefore necessarily results in 'interceptions' because article L 244–2 actually refers to them as 'interceptions'. It is difficult to understand why no privacy rights would be implicated by these interceptions. The answer may be that privacy interests indeed are affected by the indiscriminate monitoring of radio transmissions, but that the balance between national security and privacy in this context, plus the obvious operational constraints linked to these open-ended listening activities,[48] renders any independent supervision impractical. The legality of these untargeted listening operations has to our knowledge not been tested in court.

Encryption codes communicated; DGSE uses Paris data centre

Another feature of France's Internal Security Code is the obligation for providers of encryption services to make decryption keys available to intelligence services.[49] According to *Le Monde*, France's external intelligence agency DGSE has the strongest team of encryption specialists in France, and France's computing capacity, located in a data centre in Paris, is number two in Europe, just behind the UK.[50] The *Le Monde* article quotes several sources indicating that the massive storage and analysis of data collected by the DGSE falls into a 'grey area' in the law, and that the agencies benefit from a form of 'virtual' authorization' for their data collection practices.[51]

48 As pointed out by the Minister of Justice in 1991, intelligence agencies cannot ask approval beforehand or be subject to supervision 'by reason of its technical characteristics.' Statement of French Minister of Justice (n 39). What the Minister probably meant is that intelligence agencies cannot ask for an authorization in advance because they do not know in advance to whom they may be listening during their general surveillance activities.

49 Article L 244–1, Internal Security Code.

50 Jacques Follorou and Franck Johannès, 'Révélations sur le Big Brother français', *Le Monde*, 5 July 2013.

51 *Id.*

Table 1. Summary of French mechanisms for government access to data

Kind of request	Supervision by court or independent authority	Legal provision
Requests for data in criminal investigations	Requests for data are issued by judicial police or prosecutor, without court approval, during preliminary investigations, thereafter by investigating magistrate. Requests can extend to data stored outside France. Data subjects not necessarily informed.	French Code of Criminal Procedure, 57–1, 60–2 1, 77–1–1, 77–1–2, 94 and 97.
Requests for data in customs investigations (tax, money laundering, smuggling)	Requests for data issued by customs officer without court approval.	French Customs Code, article 65.
Organized crime investigations	Police may 'clone' computers at a distance, but requires court authorization.	French Code of Criminal Procedure, article 706–102–1.
Access to traffic data and identification data in connection with national security investigations	Ministry of Defence, Ministry of Interior must go through Prime Minister's office (approx. 34,000 per year). CNCIS informed afterwards.	French Internal Security Code, articles L 246-1 through L 246-5.
Access to traffic data 'in preparation for' national security interception	Ministry of Defence and Ministry of Interior must go through Prime Minister's office first, but no prior involvement of CNCIS (approx. 200,000 requests per year)	French Code of Internal Security, article L 244–2.
Security interceptions	Ministry of Defence Ministry of Interior must go through Prime Minister's office first. CNCIS informed afterwards within 48 hours.	French Internal Security Code, article L 241—2.
General monitoring of radio transmission for 'defence of national interests'	No independent supervision.	French Internal Security Code, article L 241–3.
Access to documents necessary for untargeted 'monitoring of radio transmissions'	Ministry of Defence and Ministry of Interior may go directly to telecoms operators to request data. No supervision by CNCIS or by Prime Minister's office.	French Code of Internal Security, articles L 241–3, L 244–2.
Collection of data at listening stations outside of France	*Le Monde* reports massive data collection at listening stations outside France, and transfer of data to Paris for analysis. No supervision by court or CNCIS.	Allegedly government data collection outside of France falls outside French law. Parliamentary report recommends that the principle of non-applicability of French law be confirmed in a new law.

doi:10.1093/idpl/ipt028